# Cloud Security Services Architecture
# Version 1.2 (March 1, 2011)

| |
|---|
| **Application** |
| 1. Application-specific Identity/Authentication Service<br>2. Application-specific Authorization/Access Control Service<br>3. Provisioning Service (Identity & Access Data)<br>4. Vulnerability Assessment (Code Reviews) |
| **Virtual Machines** |
| 1. Virtual Firewall<br>2. Anti Malware<br>3. VM Configuration APIs (CPU, Memory, O/S choices)<br>4. Secure VM Access (VPN, SSH ) |
| **Hypervisor** |
| 1. Virtual Networking (VLAN – for Virtual Network Isolation (e.g., Prod, Dev etc)<br>2. Console Protection<br>3. VM Management APIs (Portability, State Control) |
| **Operating System** |
| 1. Patch Management<br>2. Anti Malware |
| **Hardware (Server)** |
| 1. (Host-based) IPS/IDS<br>2.Secure Hardware (e.g., TPM) |
| **Hardware (Storage) & Data** |
| 1. Data (at rest) Encryption<br>2. Key Management<br>3. Media Protection<br>4. Security for Data(Block) Level APIs & File APIs<br>5. Data Loss Prevention<br>6. Data Privacy Services (Retention, Destruction)<br>7. Data Backup, Restore, Archival and Preservation Services |
| **Network** |
| 1. Secure Remote Access (VPN, Radius)<br>2. Network-based Authentication (Single Sign-on) & Authorization (using Directories)<br>3. Isolation/Network Segmentation (Firewall, DMZ)<br>4. Intrusion Prevention/Intrusion Detection (IPS/IDS)<br>5. Secure Transport Services (TLS, IPSec)<br>6. Secure Messaging (Encrypted, Signed)<br>7. Secure Discovery Service (DNSSEC) |

**As an Independent (External) Service**

1. Federated Identity/Authentication Service

**Multi-layer Security Services**

1. Securing Management/Monitoring APIs
2. Audit (System Access, Transaction, Data)
3. Load Balancing/Fail over Service (for improving availability)
4. Incident Handling/Response
5. Forensics